Journal of Al-Farabi for Humanity Sciences Volume (9) Issue (6) June (2026)

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://iasj.rdd.edu.iq/journals/journal/view/95
مجلة الفارابي للعلوم الإنسانية تصدرها جامعة الفارابي

التنافس الامريكي – الصيني في الفضاء السيبراني

أ.م. د. عمر عبد الله عفتان
جامعة كلكامش كلية العلوم السياسية
أ.م.د. جنان خزعل عبد الرزاق
جامعة بغداد كلية علوم الهندسة الزراعية

The American–Chinese Competition in Cyberspace

Dr. Omar Abdullah Aftan
dromarabdullah0@gmail.com
Jenan.khazal@coagri.uobaghdad.edu.iq

الملخص

اختصر الفضاء السيبراني حاجز الزمان والمكان وخلق مساحات جديدة للتفاعلات الداخلية والدولية ونقل العلاقات الدولية الى الواقع الافتراضي، ومن ثم أدى الى تغيير في طبيعة الظواهر الدولية بما يتلائم وطبيعة هذا المجال الجديد والعوامل المفسرة لظاهرة التنافس الدولي بين الولايات المتحدة الامريكية – والصين ولم تكن الطبيعة الخاصة للفضاء السيبراني مانعاً امام استخدام ذات المحددات لتفسير التنافس بين الولايات المتحدة والصين في هذا الواقع الافتراضي، إذ ان الفضاء السيبراني ليس مجالاً منفصلاً عن باقي المجالات في الارض والجو والبحر والفضاء الخارجي، وإنما يتشابك معها ويعكس طبيعته الخاصة على كل الابعاد المفسرة لظاهرة التنافس الدولي.

الكلمات المفتاحية: الفضاء السيبراني – الولايات المتحدة – الصين – التنافس.

Abstract

Cyberspace has transcended the barriers of time and space, creating new spaces for domestic and international interactions and transferring international relations into the virtual realm. This has led to a shift in the nature of international phenomena, aligning them with the characteristics of this new domain and the factors explaining the phenomenon of international competition between the United States and China. The unique nature of cyberspace does not preclude the application of the same parameters to explain this US-China competition within this virtual reality. Cyberspace is not a separate domain from other domains on land, in the air, at sea, and in outer space; rather, it is intertwined with them, reflecting its unique nature across all dimensions that explain the phenomenon of international competition.

Keywords: Cyberspace – United States – China – Competition

المقدمة

الفضاء السيبراني عصب الحياة البشرية وشريانها ومصدر طاقتها وترابطها، وارتبط ظهوره بظهور الانترنت ومواقع الويب، وكون بيئة من صنع الانسان، تتسم بسهولة استخدامها ورخص تكلفتها وقيامها بأدوار مختلفة في الحياة البشرية سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية، ولم تعد تلك البيئة حكراً على الدول فقط، بل من يمتلك أليات توظيف هذه البيئة السيبرانية الجديدة يصبح الأكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة، ولانعكاس الفضاء السيراني على المحددات المادية وغير المادية للتنافس عدة مظاهر في كل الابعاد المذكورة تساعد على فهم التنافس السيرابي الامريكي – الصيني. تعد كل من الولايات المتحدة والصين التفوق التكنولوجي القضاء السيبراني أساساً للقوة الاقتصادية والعسكرية، ومن ثم أساساً لمكانتهم في النظام الدولي.

هدف البحث: تسليط الضوء على علاقة امريكا والصين في الفضاء السيبراني كون العلاقة معقدة وتتضمن تنافساً استراتيجيا، حيث تسعى كل دولة لحماية بنيتها التحتية وتطوير قدراتها السيبرانية.

اشكالية البحث: تنطلق من سؤال مركزي هو وجود اتهامات متبادله بالتجسس والهجمات السيبرانية خاصة في ما يتعلق بالابتكار التكنولوجي والشبكات والذكاء الاصطناعي وتأثير ذلك على الا من القومي لكلا البلدين وانتهاك الخصوصية.

منهجية البحث: اعتمد البحث على منهج المصلحة الوطنية ومنهج التحليل النظمي من خلال دراسة الأسباب التي أثرت على العلاقة بين البلدين في مجال الأمن السيبراني.

فرضية البحث: تنطلق فرضية البحث من التنافس الامريكي – الصيني في العلاقات الدولية وخاصة في هذا المجال مع التطور التكنولوجي المتسارع.

هيكلية البحث: تم تقسيم البحث إلى مبحثين تناول المبحث الأول: البعد الجيوسياسي للتنافس الأمريكي – الصيني في الفضاء السيبراني، وتناول المبحث الثاني: البعد العسكري والأمني للتنافس الامريكي – الصيني في الفضاء السيبراني.

المبحث الأول البعد الجيوسياسي للتنافس الامريكي □ الصيني في الفضاء السيبراني

يمكننا الربط بين البعد الجيوسياسي والجيواستراتيجي والتنافس السيبراني بين الولايات المتحدة والصين على أكثر من جانب، وهي كالآتي:

١) منطقة التنافس في بحر الجنوب وتايوان من الأهمية بمكان، قد تكون سببا في المواجهة العسكرية مع استمرار التصعيد بين الأطراف المتنازعة الإقليمية، ولن تستطيع الولايات المتحدة الاستمرار في دورها الدبلوماسي المحايد بل قد يكون عليها تحريك المعدات العسكرية واتباع سلوكيات عدائية قد تدمر الإقليم، هذا السيناريو الأسوأ قد يسبب ضررا كبيرا على الجانبين الاقتصادي والعسكري للدولتين[١]، هذا في الواقع الحقيقي، ناهيك عن استخدام الأسلحة السيبرانية وتبادل الهجمات السيبرانية، ومن ثم هذه المنطقة تعتبر سلاحا ذا حدين؛ إما صمام أمان للمصالح أو تدمير للعالم.زاد التوتر بين الولايات المتحدة والصين بسبب محاولات الأولى توسيع نطاق وجودها في المحيط الهادي بوتيرة متسارعة، ولا سيما في جزيرة غوام" وإنشاء قاعدتين جوية وبحرية بالإضافة إلى بعض المنشآت الإستراتيجية تشارك في تدريبات ومناورات في شبه الجزيرة الكورية والمناطق المجاورة لها؛ مما أثار الغضب الصيني، أسفر ذلك عن هجمات سيبرانية بواسطة مجموعة يطلق عليها فولت تايفون، ونشرت عنها مايكروسوفت أنها استهدفت عددًا من البني التحتية الحيوية في جزيرة غوام[٢]، وكانت وكالة الأمن القومي قد اكتشفت تلك الهجمات، كما كشفت مايكروسوفت عن شبكة واسعة حاولت التوغل عبر قطاعات متعددة مثل النقل الجوي والاتصالات والنقل البحري والبري.ولكن نفت الصين الاتهامات التي وجهت إليها بشن هجمات سيبرانية أو تنفيذ عمليات تجسس على كيانات أمريكية في المنطقة أو غيرها، كذلك اتهمت الولايات المتحدة وحلفاؤها الصين بالقرصنة واسعة النطاق التي استهدفت خدمات "مايكروسوفت اكستشانج للمراسلة، وقوبل هذا العمل أيضًا بالإنكار من الجانب الصيني.بدأ شي جين بينغ انتقاد سياسة الولايات المتحدة الأمريكية ورفض الدور القيادي الأمريكي الإقليمي في عام ٢٠١٧، ودعم الخطابات القومية بسلوك استفزازي في الفضاء السيبراني، ووضعت الحكومة الصينية سباق القيادة السيبرانية مع الولايات المتحدة بحلول عام ٢٠٤٩، وبدأت في تكثيف الجهود لتطوير بنيتها التحتية العالمية ومنها الاستقلال عن نظام GPS أو نظام التموضع العالمي للملاحة" وكابلات الاتصالات البحرية، ويصبح جليًا خطة الصين للوصول إلى التوازن التنافسي في المرحلة المقبلة، وأصبح كل من عسكرة بحر الصين الجنوبي والهجمات السيبرانية الدورية على أهداف أمريكية تهديدًا للهيمنة الأمريكية[٣]. واتسمت تلك المرحلة بانتهاء الممارسات الأمريكية طويلة الأمد الحذرة والمراعية للعلاقات مع الصين وفرض المزيد من القيود على الصين، وظهر ذلك جليًا في حظر البيت الأبيض التعامل مع شركة هواوي عملاق التكنولوجيا الصينية وإصدار وثيقة بعنوان النهج الإستراتيجي للولايات المتحدة تجاه جمهورية الصين الشعبية.

٢) قد تساعد التحالفات الإقليمية بين الدول الآسيوية والولايات المتحدة ضد الصين، في عرقلة تطبيق الصين لتكنولوجيا الجيل الخامس في شرق آسيا في الدول الحليفة، كما قد يساعد خلق التوترات في المنطقة بمزيد من الهجمات السيبرانية وتهديد الأمن السيبراني للدول الإقليمية في منطقة بحر الصين الجنوبي والولايات المتحدة على السواء من جانب الصين إن لم تفكر في الخيار العسكري.

من جهة أخرى عملت الولايات المتحدة على تعزيز البنية التحتية الرقمية الآمنة وتنوع خدمات الاتصالات، وتعميق المرونة المشتركة في الشبكات الحكومية والبنية التحتية الحيوية، مع بناء مبادرات إقليمية جديدة لتحسين الأمن السيبراني الجماعي والاستجابة السريعة للحوادث السيبرانية، وساعد في ذلك تعميق العلاقات مع اليابان وكوريا الجنوبية[٤].

٣) أنشأت الصين إستراتيجية بحرية للسيطرة على طرق المواصلات والممرات واستغلال ثرواتها لتقوية الاستثمار بمجال البحث والتطوير في صناعة أشباه الموصلات؛ حيث إن هذه المنطقة غنية بالرمال التي تدخل في صناعتها ، وصناعة الأسلحة المتقدمة كحاملات الطائرات والأسلحة النووية والأقمار الصناعية وتكنولوجيا الاتصال العسكري وأنظمة القيادة والسيطرة على بحر الصين الجنوبي وخلق عقيدة ترتكز على الكيف أكثر من الكم للاقتراب من إمكانيات الولايات المتحدة وقدراتها بحلول عام ٢٠٥٠.

٤) تعد سيطرة تايوان على صناعة أشباه الموصلات الحيوية في العالم تعزيزا للقوة الاقتصادية الصينية، ولا سيما في تطوير تكنولوجيا الجيل الخامس، كذلك القيمة الإستراتيجية الضخمة في سلسلة التوريد العالمية للرقائق الإلكترونية فائقة التقدم تعد سببًا قويًا جدًا وسلاحًا تستخدمه الولايات المتحدة لإبقاء الصين بعيدة عن تايوان، لذلك تلك الأخيرة تمثل في حد ذاتها رادعا أمام قيام الصين باللجوء للقوة تجاهها[٥].وكمحاولة لتهديد الولايات المتحدة ووقف دعمها لتايوان فرضت الصين عقوبات اقتصادية وتجارية على أكثر من ١٠٠ شركة أغذية في تايوان وتعليق تصدير الرمال الطبيعية وهو المكون الرئيسي الذي يدخل في صناعة الرقائق وأشباه الموصلات التي تشكل أهمية كبيرة للاقتصاد التايواني؛ حيث تستهلك ٩٠ مليون طن متري من الرمال الطبيعية في العام ثلثها من الصين.يتضح أن قضية تايوان هي عنوان المنافسة الجيوسياسية ولها أثرها في التطور التكنولوجي الحالي، إن تايوان هي الرائدة في توريد رقائق أشباه الموصلات وبها أكبر شركة لإنتاج الرقائق TSMC التي تنتج ٩٠٪ من إجمالي الطلب العالمي من الرقائق الالكترونية التي تدخل في صناعة الهواتف وأجهزة الكمبيوتر والسيارات والطائرات المدنية والعسكرية في العالم، ويطلقون عليها اسم الجبل المقدس، وتتسبب تلك الصناعة في التوتر الدائر بين الولايات المتحدة والصين وأصبح مصير تلك الصناعة مصدر قلق عالمي، وتعد تلك الصناعة مؤثرة في الأجهزة التكنولوجية من أجهزة الكمبيوتر إلى الأسلحة المتقدمة، وكان لوباء كورونا أثر في هذه الصناعة من قبل، وإذا وقع الصراع سيكون كارثيا ليس فقط على تايوان ولا على الصين ولا على الولايات المتحدة ولا الاتحاد الأوروبي، بل ستحدث فوضى عالمية، فنقص الرقائق إذا سقطت تايوان في يد الصين من المحتمل أن تمنع الدول الغربية من الوصول إلى رقائق أشباه الموصلات التي لها أهمية كبيرة في التقنيات المتقدمة مثل الذكاء الاصطناعي وشبكات تكنولوجيا الجيل الخامس والسادس[٦].إن انقطاع إمدادات الرقائق التايوانية لمدة عام واحد سيكلف شركات التكنولوجيا العالمية (ومنها هواوي) ما يقرب من ٦٠٠ مليار دولار ، لذلك لجأت الولايات المتحدة إلى هذه الوسيلة كنوع من الضغط على الصين في حربها التجارية معها وتصعيدها ضد شركة هواوي لمنع تطبيق تكنولوجيا الجيل الخامس وحظر معداتها في العالم. وتسببت أزمة الرقاقات الرقمية في حرب سرية سيبرانية بين الولايات المتحدة والصين تارة بالتجسس وتارة بالهجمات السيبرانية التي يتهم فيها كل طرف الآخر.

٥) وكما تحدثنا في سياق البعد الجيوسياسي عن تمسك الصين بالسيادة الوطنية والإقليمية ومدى حساسية المنطقة لها، لذا فهي من أهم القضايا الخلافية بينها وبين الولايات المتحدة، عند الانتقال إلى الفضاء السيبراني أيضا تظهر أهمية السيادة السيبرانية، فما نجد كثيرا من الأبحاث تحدثت عن السيادة السيبرانية وأهمية السيطرة عليها لأنها تؤثر تأثيرًا مباشرًا في السيادة الوطنية والإقليمية، إلا أننا نلاحظ وجود تناقض بين السيادة السيبرانية وفكرة الإنترنت القائمة على الوحدة والاتصال البيني غير المقيد والتركيز على السيادة السيبرانية وتحكم الدولة سوف يخلق فضاء سيبرانيا لكل دولة منفصلا عن الأخرى مما يؤدي إلى تجزئة الإنترنت[٧].في الوقت الذي تنادي فيه الصين بالسيادة السيبرانية، ترى الولايات المتحدة أن تلك السيادة ليست إلا محاولة لإضفاء الشرعية على الرقابة وتوسيع نطاق سيطرة الحكومة على المجال الحر، لذلك سعت الولايات المتحدة إلى صياغة وإدارة معايير الإنترنت للمنظمات الدولية ورفضت تدويل الوظائف ذات الصلة، أو التنازل عن السلطة لوكالة متخصصة تابعة للأمم المتحدة. كما أخذت على إقناع دول المنطقة الحليفة بنظم جماعية لحماية وأمن البنى التحتية الخاصة بها، وهذا كله ترفضه الصين.أشار الكتاب الأبيض للصين في عام ٢٠١٠ إلى أن الإنترنت الذي يتدفق إلى الأراضي الصينية، يجب أن يخضع لسيادة الدولة الصينية وينبغي احترام سيادة الإنترنت في الصين، وفي عام ٢٠١٤ أعرب الرئيس الصيني شي جين بينج عن استعداد الصين للعمل مع جميع بلدان العالم لتعميق التعاون الدولي واحترام سيادة الإنترنت والسلام والأمن والشفافية في الفضاء السيبراني، وفي ديسمبر عام ٢٠١٥ صرح الرئيس الصيني في حفل افتتاح المؤتمر العالمي الثاني للإنترنت": (يجب تشجيع الالتزام العالي باحترام السيادة السيبرانية والمشاركة المتساوية في الشبكات الدولية، ضمان الحق في الفضاء السيبراني، وعدم الانخراط في الهيمنة السيبرانية وعدم التدخل في الشئون الداخلية والأنشطة السيبرانية للبلدان الأخرى أو دعم الممارسات التي تعرض أمن الدولة للخطر، بالنسبة إلى الصين فإن الأمن السيبراني جزء من السيادة السيبرانية ويرتبط مفهوم السيادة السيبرانية بالحاجة إلى التحكم في أي نشاط يرتبط بالدولة والأمة والحزب، فالحكومة الصينية تعمل على تركيز الرقابة والتحكم في الإنترنت ومحتواه) [٨].على الجانب السياسي والجيوسياسي سعت الدولة الصينية إلى نفوذ أكبر بشأن حوكمة الفضاء السيبراني، وصاغت عدة مواقف تجاه إدارة الإنترنت العالمية

التي تمثل تحديا واضحًا للتنظيم الذي تهيمن عليه الولايات المتحدة الأمريكية، ترى وجهة النظر الأمريكية أن تعدد أصحاب المصلحة في قيادة الإنترنت يجلب الفائدة الاقتصادية والعسكرية والاستخباراتية للولايات المتحدة نفسها وحلفائها، ولكن تدعو الصين إلى نموذج متعدد الأطراف وتدويل الحوكمة" تحت راية الأمم المتحدة وتمكين الدول النامية[٩].سيطرت ما يسمى بـ"السيادة السيبرانية على الإدارة الصينية الحالية حيث يتم إجراء بعض التغييرات الاستباقية من خلال الكيانات المركزية المنظمة المبادرات الإستراتيجية، الكتابات السياسية، وفي عام ٢٠١٤ تحت القيادة المباشرة للرئيس شي جين بينغ" ورئيس الوزراء لي كه تشيانغ" تم إنشاء "المجموعة القيادية المركزية لأمن الإنترنت والمعلومات" التي تغيَّر اسمها فيما بعد إلى اللجنة المركزية لشئون الفضاء السيبراني"، وتم الترويج لجدول أعمال السيادة السيبرانية استجابة للتأثيرات المعقدة الخارجية المتنازعة من الكيانات فوق الوطنية والبنى التحتية للشركات والسياسات الشبكية.يخضع الإنترنت داخل الأراضي الصينية إلى سيادة السلطة القضائية الصينية التي لا بد من احترامها وحمايتها، وفي عام ٢٠١٥ أشير إلى مزيد من التفاصيل في المؤتمر العالمي الثاني للإنترنت "لا بد من احترام حق كل دولة في اختيارها لطريق التطوير السيبراني بشكل مستقل، نموذج التنظيم السيبراني، والسياسات العامة للإنترنت، وتشارك في حوكمة الفضاء السيبراني الدولي على قدم المساواة"[١٠].لطرح خطاب السيادة على الإنترنت، تعمل الصين بشكل وثيق مع الوحدات الجيوسياسية الناشئة وأغلبها من الأقاليم التاريخية المحيطة وشبه المحيطة من خلال الشراكات الإستراتيجية وتشمل "منظمة شانغهاي للتعاون"، "مؤتمر Wuzhen العالمي للإنترنت"، مبادرة الحزام والطريق منتدى التعاون الصيني الإفريقي ، و "CyberBRICS في هذا التعاون، فإن المنهج المزدوج في التوسع الصيني في الصناعة الرقمية وبناء التحالفات للحوكمة السيبرانية مرئي للجميع، والنمو الصيني للرأس المال الخاص بالإنترنت والرغبة في قيادة تنظيم بديل، من شأنه أن يشكّل تهديدًا للقوة الجيوسياسية والاقتصادية للولايات المتحدة[١١].ومع تغيير مفهوم القوة في العالم ولا سيما القوة العسكرية التقليدية، ومع تغيير سياسة سباق التسلح إلى سباق تسلح من النوع السيبراني واستمرار استعراض القدرات العسكرية ولا سيما في بحر الصين الجنوبي، دخلت القوة السيبرانية والهجمات السيبرانية لتشارك بدورها كل ما هو تقليدي محاولة تأدية الدور الذي يساعد في تسوية النزاعات في هذه المنطقة (خاملة البركان). لذلك ننتقل إلى استعراض أهم سمات البعد العسكري والأمني للتنافس السيبراني الأمريكي– الصيني في السياق التالي:

المبحث الثاني البعد العسكري والأمني للتنافس الأمريكي الصيني في الفضاء السيبراني

شكلت القفزة التكنولوجية في مجال الاتصال والمعلومات مفاهيم جديدة كبروز الفضاء السيبراني وأسهمت في تحول ديناميات التفاعل في عالمنا الراهن وتغيير مفهوم القوة ليصبح التركيز في القدرة على التأثير في مسارات تدفق المعلومات والاتصالات في الفضاء السيبراني، ويشكّل ذلك معيارا لتقدم الدول، هذا ما أسهم في زيادة وعي وإدراك القوى الكبرى بأهمية تأثير العامل التكنولوجي والمعلومات في بنية موازين القوى العالمية والتحول من معيار القوة الصلبة والناعمة والقوة الذكية إلى القوة السيبرانية.ويتناول مفهوم القوة السيبرانية كل قضايا التفاعلات الدولية المادية وغير المادية على حد سواء. وتعطي القوة السيبرانية دافعًا قويًا في اتجاهين؛ الأول تدعيم القوة الناعمة؛ حيث بات الفضاء السيبراني مسرحًا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة والحرب النفسية والتأثير في توجهات الرأي العام والنشاط السري والاستخباراتي، أما الاتجاه الآخر، فيتعلق بتبني الدول لزيادة الإنفاق في سياسات الدفاع السيبراني وحماية شبكاتها الوطنية من خطر التهديد وبناء مؤسسات وطنية للحماية السيبرانية[١٢].وكان للفضاء السيبراني دور كبير في تغيير طبيعة تفاعلات السياسات العالمية، وكما ظهر نوع جديد من القوة هو "القوة "السيبرانية ظهر نوع جديد من الأمن هو "الأمن السيبراني"، ونوع جديد من الردع "الردع السيبراني"، ونوع جديد من سباق التسلح سباق التسلح السيبراني"، وبالمعنى الافتراضي في الفضاء السيبراني أصبح الهدف تعظيم القوة السيبرانية وتحول التنافس إلى تنافس على الموارد السيبرانية، التي سوف يتحدد من خلال اكتسابها أو فقدها الموقع النسبي للدولة وزيادة التنافس حول هذه القوة يرتبط بالنمو السريع للفضاء السيبراني. ويطرح جوزيف ناي أربعة تهديدات على الأمن القومي للدول وهي: التجسس الاقتصادي، والجريمة الإلكترونية، والحرب السيبرانية، والإرهاب السيبراني[١٣]

ويرجع أسباب اهتمام الفاعلين من الدول أو غير الدول بتحقيق الهيمنة من خلال امتلاكها لعدة سمات منها:

١) ساحة صراع افتراضية حيث يتخطى الفضاء السيبراني العديد من الثنائيات التي في الصراعات التقليدية، وهو أقل تكلفة من حيث الخسائر المادية وأكثر تحديدًا للهدف.

٢) زيادة الاعتماد السيبراني: حيث باتت الدول تربط بنيتها التحتية بالفضاء السيبراني خاصة شبكات الكهرباء والمياه والبنوك والاتصالات وجمع المعلومات.

٣) صعوبة وضع حدود زيادة حالة التأثير الشبكي داخل الدول وخارجها، واتساع استخدام التكنولوجيا الحديثة المرتبطة بالفضاء السيبراني.

ولاستخدام القوة داخل الفضاء السيبراني عدة أنماط منها:

١) الحرمان من الخدمة وإدخال البرامج الضارة أو حملة المعلومات وتجنيد أعضاء المنظمات الإرهابية.

٢) الضغط على الشركات لاستيعاب الأفكار التي تخص البرامج المقبولة.

٣) تهديدات بمعاقبة المدونين الذين ينشرون مواد خاضعة للرقابة على مواقع الإنترنت.

ويقسم النشاط السيبراني إلى ثلاث فئات، وهي الأضرار المادية للممتلكات، وقطع نظام تدفق المعلومات، وعمليات الوصول للهدف.

١) القدرات العسكرية السيبرانية للولايات المتحدة والصين:

وتعد الصين والولايات المتحدة من أكبر القوى في مجال الاستحواذ على القوة السيبرانية القادرة على توفير أقصى درجات الأمن السيبراني، ويطلق عليها القوى السيبرانية العظمى "Cyber Superpower" وفي ظل هذه التغييرات التكنولوجية وظهور الفضاء السيبراني كساحة جديدة للتفاعلات أصبح الأمن السيبراني تحديًا عالميًّا يهدد الأمن القومي للدول.

أنشأت بعض الدول ومنها الولايات المتحدة والصين كتائب أو جيوش من القراصنة الإلكترونيين، حيث وجدت فيها وسيلة للمساهمة في تحقيق أهداف الدولة الإستراتيجية مثل محاولة اختراق الأنظمة الإلكترونية للدول الأخرى وسرقة البيانات والمعلومات والخطط العسكرية والإستراتيجية والدفاع عن الشبكات الوطنية للدولة ضد أي محاولة اختراق خارجية، كذلك يوجد اتجاه متزايد لإنشاء وحدات خاصة بالحروب السيبرانية التي تتم عبر الفضاء السيبراني، ومن أبرز تلك الوحدات الوحدة ٦١٣٩٨ في الصين، والقيادة العسكرية cyber command US في الولايات المتحدة(١٤).

أ) الوحدة ٦١٣٩٨:

هي وحدة سرية بجيش التحرير الشعبي الصيني تعتمد على شبكة من القراصنة الإلكترونيين الصينيين، تمتلك أكثر من ١٠٠ جهاز كمبيوتر مخصصة لغرض العمليات السيبرانية، في ١٣ دولة ويقع معظمها في الولايات المتحدة، وتقوم الوحدة بعمليات التجسس السيبراني وسرقة المعلومات الاقتصادية وتتسم عملياتها بالسرية التامة.وأكدت شركة "مانديات" الخاصة بالأمن السيبراني في تقرير أن الوحدة ٦١٣٩٨ بدأت في شن أولى هجماتها عام ٢٠٠٦ ، وسرقت مئات التيرابيتس الخاصة من ١٤١ منظمة تشمل المخططات التكنولوجية وعمليات التصنيع والبيانات والوثائق وخطط التسعير والتسويق ورسائل البريد الإلكتروني وقوائم الاتصال على الأقل منها ١١٥ في الولايات المتحدة، وحسب التقرير يعتقد أن الوحدة تحت إدارة المكتب الثاني التابع للإدارة الثانية لهيئة أركان جيش التحرير الشعبي، وتقع في منطقة شنغهاي"، وتمدها شركة الاتصالات الصينية بنوع خاص من الألياف الضوئية لنقل بيانات الإنترنت، ويعتقد التقرير أيضًا أن الوحدة تضم أو أنها نفسها تشكل ما يطلق عليه APT أو Advanced Persistent threat التهديد المستمر المتقدم(١٥).في ١٨ فبراير ٢٠١٣ أصدرت المخابرات المركزية الأمريكية تقريرًا من ٦٠ صفحة يتهم فيه الوحدة ٦١٣٩٨ بعمليات للتجسس والتخريب على الإنترنت، وفي ١٩ مايو ٢٠١٤ ولأول مرة في التاريخ وجه المدعي العام الأمريكي إريك " هولدر باسم مكتب التحقيقات الفيدرالي تهما جنائية بسرقة معلومات تجارية حساسة من خمس شركات أمريكية كبرى (يو إس ستيل، ألكو، ويستنكهاوس، سولار ورلد، إلى خمسة ضباط في الوحدة، وطلب من الحكومة الصينية تسليمهم للولايات المتحدة، ولكن دائمًا ما تواجه الصين الاتهامات الموجهة إليها من القيام بهجمات سيبرانية أو سرقة معلومات سرية بالنفي والادعاء بأنها تقع أيضًا ضحية لعمليات القرصنة من الدول الأخرى ومن الولايات المتحدة على الأخص.

ب) الفرق PLA3 و PLA4 الصينية:

تمتلك الصين فرقا عسكرية في العالم الرقمي، تقوم على اختراق أنظمة الاتصالات وشبكات الكمبيوتر حول العالم عامة وفي الداخل الأمريكي خاصةً ، وتمتلك الاستخبارات الصينية قطاعين متخصصين في سرقة التكنولوجيا العسكرية القطاع الأول ويدعى PLA3 الذي تخصص في سرقة التكنولوجيا العسكرية الأمريكية من خلال الهجمات السيبرانية، والقطاع الثاني يسمى الدائرة الثانية في إدارة الأركان العامة أو PLA4 الذي يقوم بمهام التجسس والاختراق السيبراني(١٦).

ج) برنامج بويزن إيفي:

نشرت صحيفة "واشنطن بوست" في تقرير لها أنباء حول محاولة الاستخبارات الصينية شراء برنامج بويزن إيفي" من إحدى شركات الأمن السيبراني الصينية، ويعرف عن هذا البرنامج أنه الأفضل لدى الجيش الصيني لدوره في الاختراق السيبراني، ويستخدم في جمع المعلومات والسبب في انتشار استخدام هذا البرنامج أن كل الأجهزة التي تعمل على أنظمة ويندوز تعتبر فريسة سهلة له وبمجرد الدخول للجهاز عن طريق البرنامج، فإنه يمكن التقاط صور وفيديوهات ونقل ملفات وسرقة كلمات سر .. ... إلخ.

د) من أهم القدرات السيبرانية الصينية مجموعات القوة السيبرانية (ATP) التي تنسب نشاطها إلى الحكومة الصينية، التي هي جزء من النشاط الحكومي السيبراني، التي عملت على إثارة البلبلة فيما يتعلق بجائحة كورونا.هـ) في عام ٢٠١٥ قام الجيش الشعبي الصيني بالهيكلة السيبرانية وتم إنشاء ثلاثة فروع دعم سيبراني جديدة؛ الأول: التعامل استخباريًا والدفاع في الفضاء السيبراني والعمليات الهجومية، والثاني: المراقبة الرقمية للأقمار الصناعية والفرع الثالث: وحدة الذكاء السيبراني، واستمرت عملية التطوير إلى أن تمت عملية الهيكلة الكاملة عام ٢٠٢٠[١٧].

و) القيادة العسكرية cyber command US:

استحدث البنتاجون في يونيو ٢٠٠٩ قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء السيبراني، وتتركز المهمة الرئيسية لهذه القيادة على حماية شبكات وزارة الدفاع وأنظمتها والاستعداد لخوض الحروب والدفاع عن شبكات الدولة الأمريكية، من خلال إدارة عمليات شبكات المعلومات التابعة لوزارة الدفاع الأمريكي لتحقيق هدفين رئيسيين، هما: حماية حرية عمل الولايات المتحدة وحرية عمل حلفائها في الفضاء السيبراني، وحرمان أعدائها من حرية العمل في الفضاء السيبراني.وقد جرى تعيين أول جنرال عسكري لإدارة حروب الفضاء السيبراني وهو "ألكسندر كيث"، وتهدف وزارة الدفاع من هذه القيادة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة سواء من حيث تأمينها أو القيام بعمليات سيبرانية عسكرية ضد أهداف خارجية، ولقد أكد وزير الدفاع الأمريكي تشاك هيجل" أنه من المتوقع أن يصل عدد قوات القيادة العسكرية للفضاء السيبراني إلى ٦٠٠٠ مقاتل عام ٢٠١٦[١٨].وقبل استحداث هذه القيادة كانت الحكومة الأمريكية تعتمد على وكالة الاستخبارات المركزية CIA ووكالة الأمن القومي الأمريكي NSA للقيام بالعمليات في الفضاء السيبراني، ومعظم مشاريع التجسس السيبراني الكبرى للولايات المتحدة مثل (PRISM) نفذتها وكالة الأمن القومي. ز – فرقة قوات الدفاع عن الشبكات العسكرية التابعة لوزارة الدفاع الأمريكية "DOD" وملحقاتها لحماية البيانات والمعلومات والتصميمات العسكرية التي تستغلها خصوم الولايات المتحدة في ترقية قدراتها العسكرية دون استنفاد أموال طائلة في بحوث التصاميم والابتكار والتطوير، مثلما تفعل الصين وفرقة قوات البعثة الوطنية للدفاع عن الولايات المتحدة الأمريكية ومصالحها ضد الهجمات السيبرانية ذات التأثيرات المدمرة وشن الهجمات السيبرانية المضادة، التي تستهدف تدمير النظم الرقمية وشبكات خصوم الجيش الأمريكي. كل دولة تسعى لاكتساب القدرات السيبرانية الدفاعية والهجومية التي أصبحت ضرورية لمواجهة تهديدات الفضاء السيبراني؛ حيث ساعد هذا الأخير في تغيير مكونات وتفاعلات النظام الدولي[١٩].

٢) مظاهر التنافس السيبراني في البعد العسكري والأمني (الدفاع والهجوم):

تزداد العلاقة بين الأمن السيبراني والأمن القومي عندما يزيد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني وخاصة مع استخدام المدن الذكية واتساع نطاق مستخدمي الإنترنت في العالم؛ مما يهدد قواعد البيانات القومية وأصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم؛ مما جعل الدول تدرك أهمية إدراج الأمن السيبراني ضمن إستراتيجية الأمن القومي.وفيما يتعلق بالهجوم، تمتاز الهجمات السيبرانية بأنها هجمات محدودة التكلفة إذا ما قورنت بهجمات عسكرية حقيقية على أرض الواقع، كما يصعب تحديد فاعلها بسبب الطابع السري لكثير من المعاملات على شبكات المعلومات[٢٠]، كما يميزها أنها لا تتقيد بالحدود الجغرافية أو المسافات، وأنها قد تتسبب في خسائر فادحة. وتستطيع هذه الهجمات أن تشل حركة الأفراد والشركات والخوادم والدول متى توفرت الإمكانات التقنية لذلك خاصة مع اعتماد المزيد من الدول على الفضاء السيبراني في تقديم الخدمات للمواطنين. وتضع الهجمات السيبرانية شرعية النظم على المحك، كما تضع أمن الدول ذاته على المحك، ولهذا كله أضحى العمل على تطوير نظم للدفاع في مواجهة هذه الهجمات هما أساسيًا من هموم المجال السيبراني.تعد الصين الخصم القوي للولايات المتحدة في الفضاء السيبراني والمجالات العسكرية التقليدية، ولم تخف طموحها للتفوق على الولايات المتحدة كقوة عالمية عظمى، وتنطلق نشاطاتها في الفضاء السيبراني منطقيًا من السعي لتحقيق هذا الهدف. وقفت بكين تعاونها في مجموعة عمل الأمن السيبراني بين الولايات المتحدة والصين "CWG" ردا على اتهامات الولايات المتحدة في يونيو ٢٠١٥ بأن هناك أدلة على أن المتسللين الصينين وراء الهجوم السيبراني على الإنترنت لمكتب إدارة شئون الموظفين وسرقة البيانات من ٢٢ مليون موظف فيدرالي حالي ورسمي[٢١].كذلك ووفق تقرير أمني صادر عام ٢٠١٥ من مؤسسة "Panda" الإسبانية والمتخصصة في مجال أمن المعلومات إلى أن نحو ٤٩٪ من أجهزة الكمبيوتر الصينية مصابة بالبرامج الأمريكية الخبيثة وهي النسبة الأكبر عالميًا، وهو الأمر الذي يضع الصين في أزمة معلوماتية حقيقية رغم الخبرات الصينية بالحرب السيبرانية وحرب الشبكات، فالقراصنة الصينيون نجحوا مرارا في مهاجمة واختراق وتجاوز الجدران النارية الشبكية وقرصنة شركات ومؤسسات التصنيع الحربي والعلمي الأمريكية.كشف القضاء الأمريكي عن توجيه اتهامات إلى أربعة قراصنة صينيين بينهم ثلاثة موظفين في وزارة أمن الدولة متهمين بالتسلل إلى أنظمة شركات وجامعات وحكومات بين ٢٠١١ و ٢٠١٨

بهدف سرقة بيانات أو تكنولوجيا.في يناير ٢٠١٩ صدر عن مكتب المخابرات الوطنية الأمريكية (DNI) تقريرا يشير إلى تصاعد أنشطة التجسس السيبراني التي تقوم بها الصين[٢٢]، ونص التقرير أن الحكومة الصينية طورت قدراتها في الهجمات السيبرانية، بما في ذلك توجيه آراء المواطنين الأمريكيين فيما يتعلق بالمشكلات القائمة المرتبطة بمنتجات شركتي "هواوي" و زد تي أي الصينيتين، إذ قال السيناتور "مارك ورنر" نائب رئيس لجنة الاستخبارات في مجلس الشيوخ الأمريكي: (إن شركتي هواوي و "زد تي أي" للاتصالات تشكلان تهديدًا للولايات المتحدة)، ودعا في بيان مشترك مع السيناتور "ماركو روبيو" العضو في اللجنة على السلطات الأمريكية إلى الاحتراس لحماية التكنولوجيا الحساسة من أنشطة التجسس الأجنبية)، كما تحذر الولايات المتحدة الغرب الأوروبي من إمكانية استخدام أنظمة ومنتجات شركات الاتصالات الصينية العملاقة لأغراض التجسس التي منها "هواوي" محل الدراسة.وأكد الخبراء الأمنيون تصاعد هجمات القراصنة الصينيين فيما يتعلق بمحاولة سرقة معلومات عن أبحاث بخصوص لقاح كورونا، واستغلال وقت الوباء لعمل هجمات على البنية التحتية، وقالت صحيفة نيويورك تايمز إن مكتب التحقيقات الفيدرالي (FBI) ووكالة الأمن القومي قدما تحذيرًا يفيد بأن المتخصصين في مجال اختراق المعلومات إلكترونيًّا العاملين لحساب الصين يسعون لسرقة المعلومات الخاصة بالأبحاث الأمريكية المخصصة لإيجاد لقاح لفيروس كورونا، من أهم مظاهر التنافي السيبراني مؤخرا بين الولايات المتحدة والصين[٢٣].

٣) محاولات معالجة التهديدات السيبرانية:

أ) محادثات مجموعة العمل السيبرانية الأمريكية – الصينية ٢٠١٣ CWG: كانت أولى تلك الجلسات في يوليو ٢٠١٣ في واشنطن بين الرئيس باراك أوباما والرئيس شي جين بينغ لاتخاذ إجراءات أكثر عملية لزيادة المناقشات الثنائية حول القواعد والمبادئ الحاكمة للفضاء السيبراني، وتقوية التعاون والتنسيق بين الولايات المتحدة والصين، وكانت تلك المجموعة بمثابة منصة مهمة لمعالجة القضايا الخلافية السيبرانية بين البلدين بشكل مستمر ومؤثر .

ب) اتفاق الانفراج السيبراني ٢٠١٥: قدم اتفاق "الانفراج السيبراني" بين الرئيس أوباما والرئيس شي جين بينغ عام ٢٠١٥، وإن لم ينجح بشكل كامل، نموذجا لمعالجة التهديدات السيبرانية بواسطة إجراءات الدفاع والردع وتتمثل من ناحية في الجهود الدفاعية: مثل تمويل عمليات تحديث التكنولوجيا، وسن قوانين تتعلق بالصناعات المتصلة بالأجزاء المحورية في البنية التحتية[٢٤]، وتحسين التعاون ومشاركة المعلومات بين الحكومة والصناعات.ومن ناحية أخرى اشتمل الردع على اتخاذ إجراءات عقابية من قبل جهات إنفاذ القانون أو فرض عقوبات ضد الجناة كأفراد أو على الوكالات الاستخباراتية والعسكرية التي يأتمرون بإمرتها.ولكن للأسف لم تسفر هذه المحاولات عن حلول حقيقية ومستمرة، لاستمرار الهجمات السيبرانية المتبادلة من الدولتين.

الخاتمة

أسهمت الثورة التكنولوجية والاعتماد على التقنيات المتطورة في ظهور مجال جديد هو الفضاء السيبراني وتغيير مفاهيم تقليدية كثيرة في العلاقات الدولية ، بل ان الفاعلين الدوليين أنفسهم أصابهم هذا التغيير ولم تعد الدولة هي الفاعل الوحيد والمؤثر في النظام الدولي، أصبح هناك شركات عابرة للحدود لديها من المقومات والقدرات الجديدة كالبيانات الضخمة والمعلومات والمعدات ما يسمح لها بالمنافسة والتأثير، وأدى هذا التطور للفضاء السيبراني الى ظهور مساحات جديدة للتفاعل تختلف عن تلك التقليدية، فاصبح لدينا قدرات سيبرانية وقوة سيبرانية تتسابق عليها الدول الكبرى وتدخل في اعادة تشكيل النظام الدولي و توازن القوى. وتتسم العلاقات الأمريكية الصينية بانها معقدة ومتشابكة. ويبدو إن واشنطن لن تسمح بأي منافسة لدورها العالمي دون تكلفة مما يثير التساؤلات حول قدرة الصين وما لديها من قوة تساعدها على مجارات الخطوات الامريكية لا سيما في مجالات القوة السيبرانية والقوة الاقتصادية والاتفاق العسكري والقوة الناعمة، ومهما اتبعت الولايات المتحدة من خطوات محددة للتعامل مع الصعود الصيني لا يمكن اغفال نجاح السياسة الصينية في استيعاب ذلك، ومن المتوقع أن تظهر الصين نجاحاً واضحاً في التعاطي مع أي ضغوط مستقبلية.

قائمة المصادر

أولاً: الكتب:

١) اسماعيل صبري مقلد، العلاقات السياسية الدولية، الكويت، جامعة الكويت، ١٩٧٩.

٢) ايهاب خليفة، مجتمع ما بعد المعلومات، القاهرة للنشر والتوزيع، ٢٠١٩.

٣) رولا حطيط، الحرب الخفية في المنطقة المظلمة، مركز الدراسات الفلسطينية والاستيراتيجية، بيروت، ٢٠٢٠.

٤) سعود احمد يحيى، الحروب السيبرانية، المجلة القانونية، جامعة القاهرة، ٢٠١٨.
٥) سمير البعلبكي، الفضاء السيبراني والعلاقات الدولية، دار العلم، بيروت، ٢٠٢١.
٦) عادل عبد الصادق، الفضاء الالكتروني والرأي العام، المكتبة الاكاديمية، القاهرة، ٢٠٢١.
٧) عادل عبد الصادق، الفضاء الالكتروني والعلاقات الدولية، القاهرة، المكتبة الاكاديمية، ٢٠١٦.
٨) عرفات ابراهيم، الصين وحواجز الصعود، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠٠٦.
٩) فوزي درويش، الشرق الأقصى – الصين واليابان، دار الكتب المصرية، القاهرة، ٢٠٠٩.
١٠)محمد جمال مظلوم، الامن غير التقليدي، جامعة نايف العربية للعلوم الأمنية، ٢٠١٢.
١١)محمد صقر، التنافس الامريكي – الصيني وانعكاساته على منقطة الشرق الأوسط، الرياض، المعهد الدولي للدراسات الايرانية، ٢٠٢١.
١٢)مصطفى كمال، جيوسياسية الطاقة النزاع الامريكي – الصيني، السياسة الدولية، مركز الاهرام، ٢٠١٩.

ثانياً: البحوث:

١) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، ٢٠١٩.
٢) أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، جامعة الامارات العربية المتحدة، ٢٠٢٠.
٣) حسين محمد علي، العلاقات الامريكية الصينية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، ٢٠٢١.
٤) شريف كلاع، التحالف الاستراتيجي الصيني – الروسي في مواجهة النظام الاحادي القطبية، مجلة افاق للعلوم، القاهرة، ٢٠٢١، ص١٨,
٥) ضياء ابراهيم، الحضور الصيني في الشرق الأوسط وأثره على الوجود الامريكي، مجلة الشرق الأوسط، ٢٠٢٣.
٦) عبد القادر محمد فهمي، حروب الفضاء الالكتروني، مجلة العلوم القانونية والسياسية، القاهرة، ٢٠١٨.
٧) عبد المالك حطاب، المنافسة الاستراتيجية بين الصين والولايات المتحدة، مجلة العلوم القانونية والسياسية، ٢٠١٩.
٨) عميري عبد الوهاب، التنافس الامريكي الصيني من خلال الهيمنة والقوة، المجلة الجزائرية للابحاث والدراسات، الجزائر، ١٩٢٢.
٩) هيو لوفات، هل ستكون الهيمنة المقبلة على الشرق الأوسط للصين، مجلة الدراسات الفلسطينية، ٢٠٢٢.

ثالثاً: الرسائل

١) سليم دحماني، اثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الامريكية انموذجاً، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، ٢٠١٨.
٢) صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، رسالة ماجستير، جامعة الشرق الأوسط، الاردن، ٢٠٢١.
٣) فريدة طاحين، تأثير القوة السيبرانية على الاستراتيجيات الامنية للدول الكبرى – دراسة حالة الصين، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، ٢٠١٨.

هوامش البحث

(١) محمد صقر، التنافس الامريكي – الصيني وانعكاساته على منقطة الشرق الأوسط، الرياض، المعهد الدولي للدراسات الايرانية، ٢٠٢١، ص٦٤.
(٢) عادل عبد الصادق، الفضاء الالكتروني والعلاقات الدولية، القاهرة، المكتبة الاكاديمية، ٢٠١٦، ص٣٢.
(٣) اسماعيل صبري مقلد، العلاقات السياسية الدولية، الكويت، جامعة الكويت، ١٩٧٩، ص٢١٢.
(٤) ايهاب خليفة، مجتمع ما بعد المعلومات، القاهرة للنشر والتوزيع، ٢٠١٩، ص٣٢.
(٥) محمد جمال مظلوم، الامن غير التقليدي، جامعة نايف العربية للعلوم الأمنية، ٢٠١٢، ص٧٨.
(٦) مصطفى كمال، جيوسياسية الطاقة النزاع الامريكي – الصيني، السياسة الدولية، مركز الاهرام، ٢٠١٩، ص٩٤.
(٧) سعود احمد يحيى، الحروب السيبرانية، المجلة القانونية، جامعة القاهرة، ٢٠١٨، ص٢٤.
(٨) رولا حطيط، الحرب الخفية في المنطقة المظلمة، مركز الدراسات الفلسطينية والاستيراتيجية، بيروت، ٢٠٢٠، ص٨.
(٩) سمير البعلبكي، الفضاء السيبراني والعلاقات الدولية، دار العلم، بيروت، ٢٠٢١، ص٢٤.

(١٠) أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، جامعة الامارات العربية المتحدة، ٢٠٢٠، ص٢٦٤.

(١١) عادل عبد الصادق، الفضاء الالكتروني والرأي العام، المكتبة الاكاديمية، القاهرة، ٢٠٢١، ص٣٢.

(١٢) عبد القادر محمد فهمي، حروب الفضاء الالكتروني، مجلة العلوم القانونية والسياسية، القاهرة، ٢٠١٨، ص٢٦.

(١٣) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، ٢٠١٩، ص٦٤٠.

(١٤) سليم دحماني، اثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الامريكية انموذجاً، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، ٢٠١٨، ص٢٢.

(١٥) صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني، رسالة ماجستير، جامعة الشرق الأوسط، الاردن، ٢٠٢١، ص٦٢.

(١٦) فريدة طاحين، تأثير القوة السيبرانية على الاستراتيجيات الامنية للدول الكبرى – دراسة حالة الصين، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٧٨.

(١٧) شريف كلاع، التحالف الاستراتيجي الصيني – الروسي في مواجهة النظام الاحادي القطبية، مجلة افاق للعلوم،

(١٨) عبد المالك حطاب، المنافسة الاستراتيجية بين الصين والولايات المتحدة، مجلة العلوم القانونية والسياسية، ٢٠١٩، ص٦٤.

(١٩) عميري عبد الوهاب، التنافس الامريكي الصيني من خلال الهيمنة والقوة، المجلة الجزائرية للابحاث والدراسات، الجزائر، ١٩٢٢، ص١٨.

(٢٠) حسين محمد علي، العلاقات الامريكية الصينية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، ٢٠٢١، ص٣٢.

(٢١) هيو لوفات، هل ستكون الهيمنة المقبلة على الشرق الأوسط للصين، مجلة الدراسات الفلسطينية، ٢٠٢٢، ص٤٤.

(٢٢) ضياء ابراهيم، الحضور الصيني في الشرق الأوسط وأثره على الوجود الامريكي، مجلة الشرق الأوسط، ٢٠٢٣، ص٤٨.

(٢٣) عرفات ابراهيم، الصين وحواجز الصعود، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠٠٦، ص٣٢.

(٢٤) فوزي درويش، الشرق الأقصى – الصين واليابان، دار الكتب المصرية، القاهرة، ٢٠٠٩، ص٧٢.